

- 1 -

AUG 21 2006

PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of:)	
)	
Pantuso et al.)	Group Art Unit: 2137
)	
Application No. 10/071,586)	Examiner: Callahan, Paul
)	
Filed: 02/08/2002)	Date: August 21, 2006
)	
For: SYSTEM, METHOD AND)	
COMPUTER PROGRAM PRODUCT FOR)	
A FIREWALL SUMMARY INTERFACE)	
<hr/>		

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

ATTENTION: Board of Patent Appeals and Interferences

SUBSTITUTE APPEAL BRIEF (37 C.F.R. § 41.37)

This brief is in furtherance of the Notice of Appeal filed 02/03/2006, and serves as a substitute for the Appeal Brief filed 04/03/2006 in response to the Notification of Non-Compliant Appeal Brief mailed on 06/19/2006 (see attached). While appellant disagrees with the Examiner as to whether the alleged deficiencies exist in the original Appeal Brief, a Substitute Appeal Brief with appropriate edits is nevertheless submitted to expedite prosecution.

The fees required under § 1.17, and any required petition for extension of time for filing this brief and fees therefor, are dealt with in the accompanying TRANSMITTAL OF APPEAL BRIEF.

This brief contains these items under the following headings, and in the order set forth below (37 C.F.R. § 41.37(c)(i)):

- I REAL PARTY IN INTEREST
- II RELATED APPEALS AND INTERFERENCES
- III STATUS OF CLAIMS

- 2 -

- IV STATUS OF AMENDMENTS
- V SUMMARY OF CLAIMED SUBJECT MATTER
- VI GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL
- VII ARGUMENT
- VIII CLAIMS APPENDIX
- IX EVIDENCE APPENDIX
- X RELATED PROCEEDING APPENDIX

BEST AVAILABLE COPY

BEST AVAILABLE COPY

The final page of this brief bears the practitioner's signature.

- 3 -

I REAL PARTY IN INTEREST (37 C.F.R. § 41.37(c)(1)(i))

The real party in interest in this appeal is McAfee, Inc.

- 4 -

II RELATED APPEALS AND INTERFERENCES (37 C.F.R. § 41.37(c) (1)(ii))

With respect to other prior or pending appeals, interferences, or related judicial proceedings that will directly affect, or be directly affected by, or have a bearing on the Board's decision in the pending appeal, there are no other such appeals, interferences, or related judicial proceedings.

A Related Proceedings Appendix is appended hereto.

- 5 -

III STATUS OF CLAIMS (37 C.F.R. § 41.37(c) (1)(iii))

A. TOTAL NUMBER OF CLAIMS IN APPLICATION

Claims in the application are: 1-12, 19-21 and 24

B. STATUS OF ALL THE CLAIMS IN APPLICATION

1. Claims withdrawn from consideration: None
2. Claims pending: 1-12, 19-21 and 24
3. Claims allowed: 24
4. Claims rejected: 1-12, and 19-21
5. Claims cancelled: 13-18, 22-23, and 25-26

C. CLAIMS ON APPEAL

The claims on appeal are: 1-12, and 19-21

See additional status information in the Appendix of Claims.

- 6 -

IV STATUS OF AMENDMENTS (37 C.F.R. § 41.37(c)(1)(iv))

As to the status of any amendment filed subsequent to final rejection, there are no such amendments after final.

- 7 -

V SUMMARY OF CLAIMED SUBJECT MATTER (37 C.F.R. § 41.37(c)(1)(v))

With respect to a summary of Claims 1, 19, and 20, as shown in Figures 3, 6A and 6B (and the related descriptions in the specification), a system, method, and computer program product are provided for summarizing firewall activity, including various operations such as organizing a plurality of types of events associated with a firewall of a local computer (e.g. see items 104 and 106 of Figure 1, etc.) into a plurality of categories. See, for example, page 7, lines 27-30 and page 10, lines 1-8 et al. Further, various operations include tracking a number of occurrences of each type of event utilizing the firewall (e.g. see items 302 and 304 of Figure 3, etc.). In addition, various operations also include displaying a graphical representation indicating a severity of the number of the events utilizing the firewall. See, for example, page 10, lines 24-26 et al. The graphical representation includes a graph. See, for example, page 10, lines 28-30 et al. In addition, a selector is displayed for setting a blocking level of the firewall to a desired blocking level (e.g. item 602 of Figure 6A). Further, a plurality of interface features are displayed including a summary interface, an Internet protocol (IP) address interface, an event log, and a notification option interface (e.g. item 306 of Figure 3 et al.). Upon the selection of the summary interface, a recent activity list is displayed including total blocked access attempts by remote computers (e.g. item 310 of Figure 3). Upon the selection of the IP address interface, the IP address interface is displayed for selecting the IP addresses associated with the remote computers to be blocked (e.g. item 316 of Figure 3). Still yet, upon the selection of the event log, a log of the blocked access attempts by the remote computers is displayed (e.g. item 318 of Figure 3). Upon the selection of the notification option interface, a plurality of notification options is displayed for selection (e.g. see items 622 and 624 of Figure 6B, etc.). Furthermore, a lock-down option is provided for selectively blocking all access attempts via an interface (e.g. see item 602 of Figure 6A, etc.). Still yet, a user is capable of performing a visual trace (e.g. item 624 of Figure 6A), selectively blocking Internet control message protocol (ICMP) traffic, selecting the IP addresses associated with the remote computers to be allowed access, and selecting a list of application programs to be allowed to communicate over a network. See, for example, page 9, line 15 – page 11, line 27.

- 8 -

With respect to Claim 21, the above description is incorporated herein by reference. Further, included is a “means for organizing a plurality of types of events associated with a firewall of a local computer into a plurality of categories” (e.g. see items 104 and 106 of Figure 1 and page 7, lines 27-30; as well as item 400 of Figure 4 and page 11, line 29 – page 13, line 24 et al.), “means for tracking a number of occurrences of each type of event utilizing the firewall” (e.g. see items 104 and 106 of Figure 1 and page 7, lines 27-30; as well as item 400 of Figure 4 and page 11, line 29 – page 13, line 24 et al.), and “means for displaying a graphical representation indicating a severity of the number of the events utilizing the firewall, wherein the graphical representation includes a graph” (e.g. see items 104 and 106 of Figure 1 and page 7, lines 27-30; as well as item 400 of Figure 4 and page 11, line 29 – page 13, line 24 et al.).

- 9 -

**VI GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL (37 C.F.R. §
41.37(c)(1)(vi))**

Following, under each issue listed, is a concise statement setting forth the corresponding ground of rejection.

Issue # 1: The Examiner has rejected Claims 1-12, 19-21 under 35 U.S.C. 103(a) as being unpatentable over Zone Labs: "Zone Alarm Help," 6/2001, in view of S. Boran: "Personal Firewalls/Intrusion Detection Systems, An Analysis of Mini-Firewalls for Windows Users," 11/1999-12/2000, in further view of Smart Computing, "Reviews: Hack Tracer 1.2," Smart Computing, January 2001, Vol. 12 Issue 1.

- 10 -

VII ARGUMENT (37 C.F.R. § 41.37(c)(1)(vii))

The claims of the groups noted below do not stand or fall together. In the present section, appellant explains why the claims of each group are believed to be separately patentable.

Issue #1:

The Examiner has rejected Claims 1-12, 19-21 under 35 U.S.C. 103(a) as being unpatentable over Zone Labs: "Zone Alarm Help," 6/2001, in view of S. Boran: "Personal Firewalls/Intrusion Detection Systems, An Analysis of Mini-Firewalls for Windows Users," 11/1999-12/2000, in further view of Smart Computing, "Reviews: Hack Tracer 1.2," Smart Computing, January 2001, Vol. 12 Issue 1.

Group #1: Claims 1-5, 7-9 and 19-21

With respect to each of the independent claims, the Examiner has relied on Zone Labs, page 2 of "The Alerts Panel", and specifically the "Internet Alerts 3rd of 3 alerts" to make a prior art showing of appellant's claimed "tracking a number of occurrences of each type of event utilizing the firewall." Appellant respectfully asserts that such excerpt only shows a total number of alerts, but not tracking a number of occurrences of each type of event utilizing the firewall," as claimed by appellant (emphasis added).

In addition, the Examiner has relied on Zone Labs, page 1 in "Firewall Alerts" to make a prior art showing of appellant's claimed "displaying a graphical representation indicating a severity of the number of the events utilizing the firewall" (see each of the independent claims). Appellant respectfully asserts that such only discloses "an alert popup whenever [ZoneAlarm] blocks an Internet Communication." However, appellant notes that such popup does not indicate "a severity of the number of the events," as claimed by appellant (emphasis added), but only a severity of one particular event associated with the popup.

With respect to appellant's claimed technique "wherein a plurality of interface features are displayed including a summary interface" (see each of the independent claims), the Examiner has

- 11 -

relied on Zone Labs, page 5, "Alert Setting." Appellant respectfully asserts that the Alert Settings relied on by the Examiner simply relate to "sav[ing] alerts to a text file." Clearly saving alerts to a text file does not meet appellant's claimed "display[ing of a] summary interface" (emphasis added).

With respect to appellant's claimed "upon the selection of the summary interface, displaying a recent activity list including total blocked access attempts by remote computers" (see each of the independent claims), the Examiner has relied on Zone Labs, page 5 "Alert Settings: Log Alerts to a text file" and page 6, "Current Alerts." In response, appellant respectfully asserts that Zone Labs does not meet appellant's claimed "total blocked access attempts by remote computers." Zone Labs only displays each alert as it occurs, and does not specifically display "a summary interface ... displaying a ... total blocked access attempts by remote computers," as claimed by appellant (emphasis added).

With respect to appellant's claimed "upon the selection of the notification option interface, displaying a plurality of notification options for selection," the Examiner has relied on Zone Labs, page 5 "Alert Settings: Log Alerts to a text file" and page 6, "Current Alerts." Appellant respectfully asserts that such excerpts only teach allowing a user to check whether or not to "Show the alert popup window" (see Alert settings pages 5 and 6). Clearly only providing a notification option of a popup window does not meet appellant's claimed "displaying a plurality of notification options for selection" (emphasis added).

With respect to appellant's claimed technique "wherein a lock-down option is provided for selectively blocking all access attempts via an interface," the Examiner has relied on Zone Labs, "Internet Lock," page 10. Appellant respectfully asserts that the "Lock" only blocks internet traffic (see page 3), and not "all access attempts via an interface," as claimed by appellant (emphasis added).

To establish a *prima facie* case of obviousness, three basic criteria must be met. First, there must be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the reference or to combine reference teachings. Second, there must be a reasonable expectation of success. Finally, the prior

- 12 -

art reference (or references when combined) must teach or suggest all the claim limitations. The teaching or suggestion to make the claimed combination and the reasonable expectation of success must both be found in the prior art and not based on appellant's disclosure. *In re Vaecht*, 947 F.2d 488, 20 USPQ2d 1438 (Fed.Cir.1991).

Appellant respectfully asserts that at least the third element of the *prima facie* case of obviousness has not been met, since the prior art references, when combined, fail to teach or suggest all of the claim limitations, as noted above.

Group #2: Claim 6

The Examiner has relied on Zone Labs, "Alert Setting: Log Alerts to a text file" and "Current Alerts," page 6 to make a prior art showing of appellant's claimed technique "wherein the displayed number of occurrences of each type of event occurred within a predetermined time period." Specifically, the Examiner has stated that such excerpts teach that "there is kept a log file for each predetermined 24 hour period." Appellant respectfully asserts that simply nowhere does Zone Labs disclose a 24 hour period, as the Examiner contends.

Appellant respectfully asserts that at least the third element of the *prima facie* case of obviousness has not been met, since the prior art references, when combined, fail to teach or suggest all of the claim limitations, as noted above.

Group #3: Claims 10-12

The Examiner has relied on Zone Labs "Alerts," page 2 to make a prior art showing of appellant's claimed techniques "wherein a plurality of banned ports associated with the first type of the blocked attempts are displayed with the number of the occurrences associated therewith" (see Claim 10), "wherein a plurality of banned IP addresses associated with the second type of the blocked attempts are displayed with the number of the occurrences associated therewith" (see Claim 11), and "wherein a plurality of banned applications associated with the third type of the blocked attempts are displayed with the number of the occurrences associated therewith" (see Claim 12).

- 13 -

Appellant respectfully asserts that such excerpt only shows a "More Info" button with respect to a specific alert. After careful review of the Zone Labs reference, appellant notes that the "More Info Button" only "gives you access to the Alert Analyzer, located on the Zone Labs web site." However, simply nowhere does Zone Labs teach that such Alert Analyzer displays "a plurality of banned ports[, banned IP addresses and/or banned applications] associated with the first type of the blocked attempts... with the number of the occurrences associated therewith," as claimed by appellant (emphasis added). Furthermore, Zone Labs only shows a number of total alerts in the "Current Alerts" display (see "Alerts" page 2), and not a number of occurrences associated with specific types of attempts, in the manners claimed by appellant.

Appellant respectfully asserts that at least the third element of the *prima facie* case of obviousness has not been met, since the prior art references, when combined, fail to teach or suggest all of the claim limitations, as noted above.

In view of the remarks set forth hereinabove, all of the independent claims are deemed allowable, along with any claims depending therefrom.

- 14 -

VIII CLAIMS APPENDIX (37 C.F.R. § 41.37(c)(1)(viii))

The text of the claims involved in the appeal (along with associated status information) is set forth below:

1. (Previously Presented) A method for summarizing firewall activity, comprising:
 - (a) organizing a plurality of types of events associated with a firewall of a local computer into a plurality of categories;
 - (b) tracking a number of occurrences of each type of event utilizing the firewall; and
 - (c) displaying a graphical representation indicating a severity of the number of the events utilizing the firewall, wherein the graphical representation includes a graph;
wherein a selector is displayed for setting a blocking level of the firewall to a desired blocking level;
wherein a plurality of interface features are displayed including a summary interface, an Internet protocol (IP) address interface, an event log, and a notification option interface, wherein:
upon the selection of the summary interface, displaying a recent activity list including total blocked access attempts by remote computers,
upon the selection of the IP address interface, displaying the IP address interface for selecting the IP addresses associated with the remote computers to be blocked,
upon the selection of the event log, displaying a log of the blocked access attempts by the remote computers, and
upon the selection of the notification option interface, displaying a plurality of notification options for selection;
wherein a lock-down option is provided for selectively blocking all access attempts via an interface;
wherein a user is capable of performing a visual trace;
wherein the user is capable of selectively blocking Internet control message protocol (ICMP) traffic;
wherein the user is capable of selecting the IP addresses associated with the remote computers to be allowed access;
wherein the user is capable of selecting a list of application programs to be allowed to communicate over a network.

- 15 -

BEST AVAILABLE COPY

2. (Original) The method as recited in claim 1, wherein the events include blocked attempts of various types.
3. (Previously Presented) The method as recited in claim 2, wherein at least one of the types of the blocked attempts includes blocked attempts of the remote computers to access predetermined banned ports associated with the local computer.
4. (Previously Presented) The method as recited in claim 2, wherein at least one of the types of the blocked attempts includes blocked attempts of the remote computers with a predetermined set of IP addresses to access the local computer.
5. (Previously Presented) The method as recited in claim 2, wherein at least one of the types of the blocked attempts includes blocked attempts to access the network made by predetermined applications.
6. (Previously Presented) The method as recited in claim 1, wherein the displayed number of occurrences of each type of event occurred within a predetermined time period.
7. (Previously Presented) The method as recited in claim 1, and further comprising displaying additional information relating to the events upon the selection thereof.
8. (Previously Presented) The method as recited in claim 2, wherein a first type of the blocked attempts includes blocked attempts of the remote computers to access predetermined banned ports associated with the local computer, a second type of the blocked attempts includes blocked attempts of the remote computers with a predetermined set of IP addresses to access the local computer, and a third type of the blocked attempts includes blocked attempts to access the network made by predetermined applications.

- 16 -

9. (Previously Presented) The method as recited in claim 8, wherein the first type of the blocked attempts, the second type of the blocked attempts, and the third type of the blocked attempts are organized into the categories.
10. (Original) The method as recited in claim 8, wherein a plurality of banned ports associated with the first type of the blocked attempts are displayed with the number of the occurrences associated therewith.
11. (Original) The method as recited in claim 8, wherein a plurality of banned IP addresses associated with the second type of the blocked attempts are displayed with the number of the occurrences associated therewith.
12. (Original) The method as recited in claim 8, wherein a plurality of banned applications associated with the third type of the blocked attempts are displayed with the number of the occurrences associated therewith.
13. - 18. (Cancelled)
19. (Previously Presented) A computer program product embodied on a computer readable medium for summarizing firewall activity, comprising:
 - (a) computer code for organizing a plurality of types of events associated with a firewall of a local computer into a plurality of categories;
 - (b) computer code for tracking a number of occurrences of each type of event utilizing the firewall; and
 - (c) computer code for displaying a graphical representation indicating a severity of the number of the events utilizing the firewall, wherein the graphical representation includes a graph; wherein a selector is displayed for setting a blocking level of the firewall to a desired blocking level;
wherein a plurality of interface features are displayed including a summary interface, an Internet protocol (IP) address interface, an event log, and a notification option interface, wherein:
upon the selection of the summary interface, displaying a recent activity list including total blocked access attempts by remote computers,

- 17 -

upon the selection of the IP address interface, displaying the IP address interface for selecting the IP addresses associated with the remote computers to be blocked,
upon the selection of the event log, displaying a log of the blocked access attempts by the remote computers, and
upon the selection of the notification option interface, displaying a plurality of notification options for selection;
wherein a lock-down option is provided for selectively blocking all access attempts via an interface;
wherein a user is capable of performing a visual trace;
wherein the user is capable of selectively blocking Internet control message protocol (ICMP) traffic;
wherein the user is capable of selecting the IP addresses associated with the remote computers to be allowed access;
wherein the user is capable of selecting a list of application programs to be allowed to communicate over a network.

20. (Previously Presented) A system for summarizing firewall activity, comprising:
- (a) logic for organizing a plurality of types of events associated with a firewall of a local computer into a plurality of categories;
 - (b) logic for tracking a number of occurrences of each type of event utilizing the firewall;
and
 - (c) logic for displaying a graphical representation indicating a severity of the number of the events utilizing the firewall, wherein the graphical representation includes a graph;
wherein a selector is displayed for setting a blocking level of the firewall to a desired blocking level;
wherein a plurality of interface features are displayed including a summary interface, an Internet protocol (IP) address interface, an event log, and a notification option interface, wherein:
upon the selection of the summary interface, displaying a recent activity list including total blocked access attempts by remote computers,
upon the selection of the IP address interface, displaying the IP address interface for selecting the IP addresses associated with the remote computers to be blocked,

- 18 -

upon the selection of the event log, displaying a log of the blocked access attempts by the remote computers, and

upon the selection of the notification option interface, displaying a plurality of notification options for selection;

wherein a lock-down option is provided for selectively blocking all access attempts via an interface;

wherein a user is capable of performing a visual trace;

wherein the user is capable of selectively blocking Internet control message protocol (ICMP) traffic;

wherein the user is capable of selecting the IP addresses associated with the remote computers to be allowed access;

wherein the user is capable of selecting a list of application programs to be allowed to communicate over a network.

21 (Previously Presented) A system for summarizing firewall activity, comprising:

- (a) means for organizing a plurality of types of events associated with a firewall of a local computer into a plurality of categories;
- (b) means for tracking a number of occurrences of each type of event utilizing the firewall; and
- (c) means for displaying a graphical representation indicating a severity of the number of the events utilizing the firewall, wherein the graphical representation includes a graph;

wherein a selector is displayed for setting a blocking level of the firewall to a desired blocking level;

wherein a plurality of interface features are displayed including a summary interface, an Internet protocol (IP) address interface, an event log, and a notification option interface, wherein:

upon the selection of the summary interface, displaying a recent activity list including total blocked access attempts by remote computers,

upon the selection of the IP address interface, displaying the IP address interface for selecting the IP addresses associated with the remote computers to be blocked,

upon the selection of the event log, displaying a log of the blocked access attempts by the remote computers, and

- 19 -

upon the selection of the notification option interface, displaying a plurality of notification options for selection;

wherein a lock-down option is provided for selectively blocking all access attempts via an interface;

wherein a user is capable of performing a visual trace;

wherein the user is capable of selectively blocking Internet control message protocol (ICMP) traffic;

wherein the user is capable of selecting the IP addresses associated with the remote computers to be allowed access;

wherein the user is capable of selecting a list of application programs to be allowed to communicate over a network.

22. - 23. (Cancelled)

24. (Previously Presented) A firewall method, comprising:
- (a) executing a firewall in association with a local computer;
 - (b) identifying a number of blocked attempts of remote computers with a predetermined set of Internet Protocol (IP) addresses to access the local computer;
 - (c) identifying a number of attempts of the remote computers to access predetermined frequently-used ports associated with the local computer;
 - (d) identifying a number of blocked attempts to access a network made by predetermined applications on the local computer;
 - (e) displaying a menu for selecting from a plurality of interface features including a summary page, an applications page, an event log, and an IP address page;
 - (f) upon the selection of the summary page on the menu,
 - (i) displaying a recent activity list including recent activity icons corresponding to events including total blocked attempts, the attempts of the remote computers to access the predetermined frequently-used ports associated with the local computer, the blocked attempts of the remote computers with the predetermined set of IP addresses to access the local computer, the recent activity list further including a total number of the events within a predetermined time period

- 20 -

- corresponding with each recent activity icon, and a graphical representation indicating a severity of the total number of the events,
- (ii) displaying a frequently accessed port list including port icons corresponding to the predetermined frequently-used ports, the frequently accessed port list further including a total number of the attempts corresponding with each predetermined frequently-used ports, and a graphical representation indicating a severity of the total number of the attempts,
 - (iii) displaying a commonly blocked IP address list including IP address icons corresponding to banned IP addresses from which the blocked attempts of the remote computers occurred, the commonly blocked IP address list further including a total number of the blocked attempts corresponding with each IP address icon, and a graphical representation indicating a severity of the total number of the blocked attempts,
 - (iv) displaying a commonly blocked application list including application icons corresponding to banned applications associated with the blocked attempts, the commonly blocked application list further including a total number of the blocked attempts corresponding with each application icon, and a graphical representation indicating a severity of the total number of the blocked attempts;
- (g) upon the selection of the applications page on the menu, displaying an applications interface for selecting the predetermined applications;
- (h) upon the selection of the untrusted IP address page on the menu, displaying an untrusted IP address interface for selecting the IP addresses associated with remote computers to be blocked; and
- (i) upon the selection of the event log on the menu, displaying a log of the attempts; wherein a slider bar is displayed for setting a blocking level of the firewall by sliding the slider bar to a desired blocking level;
- wherein a lock-down option is provided for selectively blocking all access attempts via an interface;
- wherein a user is capable of performing a visual trace;
- wherein the user is capable of selectively blocking Internet control message protocol (ICMP) traffic;

- 21 -

wherein the user is capable of selecting the IP addresses associated with the remote computers to be allowed access;

wherein the user is capable of selecting a list of application programs to be allowed to communicate over the network.

25. – 26. (Cancelled)

- 22 -

IX EVIDENCE APPENDIX (37 C.F.R. § 41.37(c)(1)(ix))

There is no such evidence.

- 23 -

X RELATED PROCEEDING APPENDIX (37 C.F.R. § 41.37(c)(1)(x))

There is no such related proceeding.

- 24 -

In the event a telephone conversation would expedite the prosecution of this application, the Examiner may reach the undersigned at (408) 971-2573. For payment of any additional fees due in connection with the filing of this paper, the Commissioner is authorized to charge such fees to Deposit Account No. 50-1351 (Order No. NAI1P093_02.012.01).

Respectfully submitted,

By:  _____

Kevin J. Zilka

Reg. No. 41,429

Date: 8/21/06 _____

Zilka-Kotab, P.C.
P.O. Box 721120
San Jose, California 95172-1120
Telephone: (408) 971-2573
Facsimile: (408) 971-4660



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

COPY

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/071,586	02/08/2002	Joseph J. Pantano	NAI1P093/02.012.01	2679
28875	7590	06/19/2006	EXAMINER	
Zilka-Kotab, PC P.O. BOX 721120 SAN JOSE, CA 95172-1120			ART UNIT	PAPER NUMBER

DATE MAILED: 06/19/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Notification of Non-Compliant Appeal Brief (37 CFR 41.37)	Application No. 10/071,586	Applicant(s) PANTUSO ET AL	
	Examiner Paul Callahan	Art Unit 2137	

--The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

The Appeal Brief filed on 03 April 2006 is defective for failure to comply with one or more provisions of 37 CFR 41.37.

To avoid dismissal of the appeal, applicant must file an amended brief or other appropriate correction (see MPEP 1205.03) within **ONE MONTH or THIRTY DAYS** from the mailing date of this Notification, whichever is longer. **EXTENSIONS OF THIS TIME PERIOD MAY BE GRANTED UNDER 37 CFR 1.136.**

1. ☐ The brief does not contain the items required under 37 CFR 41.37(c), or the items are not under the proper heading or in the proper order.
2. ☐ The brief does not contain a statement of the status of all claims, (e.g., rejected, allowed, withdrawn, objected to, canceled), or does not identify the appealed claims (37 CFR 41.37(c)(1)(iii)).
3. ☐ At least one amendment has been filed subsequent to the final rejection, and the brief does not contain a statement of the status of each such amendment (37 CFR 41.37(c)(1)(iv)).
4. ☒ (a) The brief does not contain a concise explanation of the subject matter defined in each of the independent claims involved in the appeal, referring to the specification by page and line number and to the drawings, if any, by reference characters; and/or (b) the brief fails to: (1) identify, for each independent claim involved in the appeal and for each dependent claim argued separately, every means plus function and step plus function under 35 U.S.C. 112, sixth paragraph, and/or (2) set forth the structure, material, or acts described in the specification as corresponding to each claimed function with reference to the specification by page and line number, and to the drawings, if any, by reference characters (37 CFR 41.37(c)(1)(v)).
5. ☐ The brief does not contain a concise statement of each ground of rejection presented for review (37 CFR 41.37(c)(1)(vi)).
6. ☐ The brief does not present an argument under a separate heading for each ground of rejection on appeal (37 CFR 41.37(c)(1)(vii)).
7. ☐ The brief does not contain a correct copy of the appealed claims as an appendix thereto (37 CFR 41.37(c)(1)(viii)).
8. ☐ The brief does not contain copies of the evidence submitted under 37 CFR 1.130, 1.131, or 1.132 or of any other evidence entered by the examiner and relied upon by appellant in the appeal, along with a statement setting forth where in the record that evidence was entered by the examiner, as an appendix thereto (37 CFR 41.37(c)(1)(ix)).
9. ☐ The brief does not contain copies of the decisions rendered by a court or the Board in the proceeding identified in the Related Appeals and Interferences section of the brief as an appendix thereto (37 CFR 41.37(c)(1)(x)).
10. ☒ Other (including any explanation in support of the above items):

For claim 21, the brief fails to refer to the specification and page number in the concise explanation of the subject matter defined in the claim..

Paul Callahan
6-7-06


EMMANUEL L. MOISE
SUPERVISORY PATENT EXAMINER

AUG. 21. 2006 3:57PM
TO: USPTO

ZILKA-KOTAB, PC

NO. 3905 P. 1

ZILKA-KOTAB

PC
ZILKA, KOTAB & FEECH™

100 PARK CENTER PLAZA, SUITE 300
SAN JOSE, CA 95113

TELEPHONE (408) 971-2573
FAX (408) 971-4660

RECEIVED
CENTRAL FAX CENTER

AUG 21 2006

FAX COVER SHEET

Date: August 21, 2006	Phone Number	Fax Number
To: Board of Patent Appeals		(571) 273-8300
From: Kevin J. Zilka		

Docket No: NA11P093/02.012.01

App. No: 10/071,586

Total Number of Pages Being Transmitted, Including Cover Sheet: 30

Message:

Please deliver to the Board of Patent Appeals.

BEST AVAILABLE COPY

Thank you,

Kevin J. Zilka

☐ Original to follow Via Regular Mail ☒ Original will Not be Sent ☐ Original will follow Via Overnight Courier

The information contained in this facsimile message is attorney privileged and confidential information intended only for the use of the individual or entity named above. If the reader of this message is not the intended recipient, you are hereby notified that any dissemination, distribution or copy of this communication is strictly prohibited. If you have received this communication in error, please immediately notify us by telephone (if long distance, please call collect) and return the original message to us at the above address via the U.S. Postal Service. Thank you.

IF YOU DO NOT RECEIVE ALL PAGES OR IF YOU ENCOUNTER
ANY OTHER DIFFICULTY, PLEASE PHONE Appl
AT (408) 971-2573 AT YOUR EARLIEST CONVENIENCE

Aug 21, 2006

AUG 21 2006

Practitioner's Docket No. NAI1P093/02.012.01

PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of: Pantuso et al.

Application No.: 10/071,586

Group No.: 2137

Filed: 02/08/2002

Examiner: Callahan, Paul

For: SYSTEM, METHOD AND COMPUTER PROGRAM PRODUCT FOR A FIREWALL
SUMMARY INTERFACE

Mail Stop Appeal Briefs - Patents

Commissioner for Patents

P.O. Box 1450

Alexandria, VA 22313-1450

TRANSMITTAL OF APPEAL BRIEF
(PATENT APPLICATION-37 C.F.R. § 1.192)

1. Transmitted herewith is a substitute appeal brief which is in furtherance of the Notice of Appeal filed 02/03/2006, and serves as a substitute for the Appeal Brief filed 04/03/2006 in response to the Notification of Non-Compliant Appeal Brief mailed on 06/19/2006 (see attached).

2. STATUS OF APPLICANT

This application is on behalf of other than a small entity.

CERTIFICATION UNDER 37 C.F.R. §§ 1.8(a) and 1.10*

(When using Express Mail, the Express Mail label number is mandatory;
Express Mail certification is optional.)

I hereby certify that, on the date shown below, this correspondence is being:

MAILING

deposited with the United States Postal Service in an envelope addressed to the Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

37 C.F.R. § 1.8(a)

with sufficient postage as first class mail.

37 C.F.R. § 1.10*

as "Express Mail Post Office to Addressee"

Mailing Label No. (mandatory)

TRANSMISSION

✓ Facsimile transmitted to the Patent and Trademark Office, (571) 273-8300.

Date: 8/21/2006

April Skovmand
Signature

April Skovmand

(type or print name of person certifying)

* Only the date of filing (' 1.6) will be the date used in a patent term adjustment calculation, although the date on any certificate of mailing or transmission under ' 1.8 continues to be taken into account in determining timeliness. See ' 1.703(j). Consider "Express Mail Post Office to Addressee" (' 1.10) or facsimile transmission (' 1.6(d)) for the reply to be accorded the earliest possible filing date for patent term adjustment calculations.

Transmittal of Appeal Brief--page 1 of 2

RECEIVED
CENTRAL FAX CENTER

AUG 21 2006

3. FEE FOR FILING APPEAL BRIEF

Pursuant to 37 C.F.R. §1.17(c), the fee for filing the Appeal Brief has already been paid. However, the Commissioner is authorized to charge any fees that may be due to deposit account 50-1351 (NAI1P093).

4. EXTENSION OF TERM

The proceedings herein are for a patent application and the provisions of 37 C.F.R. § 1.136 apply.

Applicant petitions for an extension of time under 37 C.F.R. § 1.136 (fees: 37 C.F.R. § 1.17(a)(1)-(5)) for one month:

Fee: \$120.00

If an additional extension of time is required, please consider this a petition therefor.

5. TOTAL FEE DUE

The total fee due is:

Appeal Brief Fee	\$0.00 (previously paid on June 28, 2005)
Extension fee	\$120.00

TOTAL FEE DUE \$120.00

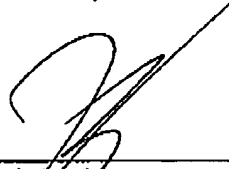
6. FEE PAYMENT

Authorization is hereby made to charge the amount of \$120.00 to Deposit Account No. 50-1351.

If any additional extension and/or fee is required, and if any additional fee for claims is required, charge Deposit Account No. 50-1351 (Order No. NAI1P093).

A duplicate of this transmittal is attached.

Reg. No.: 41,429
Tel. No.: 408-971-2573
Customer No.: 28875



Signature of Practitioner
Kevin J. Zilka
Zilka-Kotab, PC
P.O. Box 721120
San Jose, CA 95172-1120
USA

Transmittal of Appeal Brief--page 2 of 2